Deloitte & Touche Catalog of Optional Security Assessment Services

Per the contract between the State and Deloitte & Touche LLP, a set of optional security and privacy assessment services are being offered to agencies not included in the original engagement scope. We will work with the State to establish a separate scope of work for each request. We will leverage the rate card set forth in the cost proposal to determine the cost of such optional services.

Security Services	Brief Description
Security risk assessments	Assessing the security processes and controls against the security framework established for the State.
Vulnerability assessment – Infrastructure (or) Web application	Identify potential security risks on the IT infrastructure/web application, using automated vulnerability scanning tools and manual assimilation.
Vulnerability assessment – Database (or) Wireless infrastructure	Database assessment: Perform a controlled vulnerability assessment on the target database infrastructure to identify potential security vulnerabilities that may lead to unauthorized information leakage or even lead to comprise of the database system. Supported database assessments: Oracle, Microsoft SQL Server, IBM DB2, MySQL, Lotus Domino and Sybase. Wireless assessment: Identify security vulnerabilities in the configuration or implementation of the target wireless LAN infrastructure. Perform controlled discovery of wireless access nodes, high level security analysis of the configuration, and assess the overall effectiveness of the Wireless LAN infrastructure through the following tasks: • Wireless network profile • Wireless configuration and security
Cyber Threat Profile Analysis	Use leading cyber profiling practices and automation to analyze an organization's internet footprint proactively to understand how the entity looks to a cyber adversary. This includes IP WHOIS, IP Geo location, Autonomous systems, servers, addresses.
Internet Web Site Compromise Diagnostic	Utilize data gathered from the profile analysis and vulnerability assessment phases and apply Web-crawling and code-scanning techniques to find unknown malicious redirects, hosted binaries, and other compromises present.
Intranet Cyber Compromise Diagnostic	Internet-related security event logs will be analyzed to see if there is evidence of internal machines that may have been compromised and are attempting to communicate with criminal controlled devices on the Internet.

Process & Resource Assessment	An assessment will be performed against the organization's current information security processes and resources that address security incidents and cyber threats.
Confidential Data Disclosure Diagnostic	A search will be performed on Internet resources including Peer to Peer networks, criminal forums, and data stores for confidential company data.
Suspicious Program Diagnostic	Using available industry hash data sets, light-weight transient custom code will be executed on organization desktops and laptops to generate an inventory of program files.
Rogue Device Discovery Diagnostic	An analysis will be done against devices currently found in the organization's network to determine if they are rogue or exhibiting stealth-like characteristics.
Remote Access Compromise Analysis	Remote access logs are analyzed against current cyber intelligence data to expose compromised devices logging into the organization's network.
Online Application Transaction Analysis	Internet application transaction and web server logs will be analyzed against current cyber intelligence data in order to identify fraudulent transactions taking place.
Social Media Impact Survey	A policy assessment and validation will be performed to determine how social media is being used within the organization. Social networking sites will also be examined.
Business Partner Dependency Analysis	An analysis will be done to an enumerate an organization's internet sites to determine underlying dependencies and check whether the sites are currently malicious.
Cyber Security Incident Response	Resources will be dispatched to assist the organization with responding to an active or recent cyber security incident where root cause analysis is required.
Network Discovery and Perimeter Leak Test	An enterprise network discovery will be performed to identify internal hosts, routers, and subnets. Testing will also be done to check for protocol leakages at the network perimeter.
Network Security Architecture Diagnostic	An analysis of the organization's enterprise network security architecture will be performed in order to identify security weaknesses and opportunities to further reduce the risk posed by cyber criminals.
Network Firewall Architecture Design Diagnostic	An analysis will be done against the organization's network perimeter firewall design to identify weaknesses and opportunities to improve the security and performance of the architecture.
Cyber Brand Assessment	An analysis will be performed of brand related internet sites to determine if

	the brand is being improperly represented or used for fraudulent purposes.
Kiosk Cyber Security Assessment (where applicable)	An analysis will be done on kiosk deployments to determine if they are secure or being used in a fraudulent or malicious way.
Enterprise Fraud Program Assessment	An assessment will be performed of the organizations fraud program to determine if the proper skill sets, processes, organization integration, and technologies are in place to address emerging fraud issues.
Anti-Phishing Capability Diagnostic	A diagnostic will be done on the organization's anti-phishing program in order to identify gaps and improvement opportunities. It will include looking at recent phishing incidents, intelligence services, and the organization's incident handling procedures.
Insider Threat Detection Diagnostic	An assessment of the organization's insider threat detection capability including review of existing logs that can reveal current or past insider threats. The review will also assess recent incidents and recommend a roadmap for automating the capability.