Statement of Work:

Fred Cohen & Associates (FCA) will perform an Information Protection Posture Assessment (IPPA) for [CLIENT]. This will consist of the following items:

1.FCA personnel will visit the following sites:

_____
_____
_____

During these site visits FCA will hold discussions and carry out activities with key personnel to assess the information protection posture. The following activities will also be undertaken:

Facilitated discussions designed to collect information about the structure and makeup of information infrastructure at CLIENT will be undertaken and documentation will be gathered and generated to produce an overview of the CLIENT security architecture. This will include but not be limited to issues related to:

(a) Understanding of how the CLIENT and its information technology operate and what makes it succeed or fail in terms of information systems, including understanding where the business value lies and the impacts of information corruption, loss of availability, loss of control, and leakage involving different elements of information systems and infrastructure,

(b) Understanding oversight requirements and responsibilities and identifying established duties to protect, including but not limited to nature and type of company, legal requirements, owner-driven requirements, board of directors requirements, executive management requirements, and audit-driven requirements.

(c) Identifying and understanding the current risk management process including threats, vulnerabilities, and consequences associated with information and information technologies, risk tolerance as displayed by management, selection criteria for risk avoidance, acceptance, transfer, and mitigation, and association of surety to risk.

(d) Identifying the structure of information protection and its management including coverage of:

- Protection Management
- Protection Policy
- Standards and Procedures
- Documentation

- Protection Audit
- Protection Testing
- Technical Safeguards
- Personnel issues
- Physical Protection
- Incident Response
- Legal Considerations
- Training and Education
- Protection Awareness
- Organizational Issues

and covering feedback and decision-making mechanisms that support proper control of the protection function withing the organization.

(e) Understanding the current control architecture including but not limited to protection objectives, access controls, functional control units, and change management processes.

(f) Understanding technical security architecture, life cycle coverage, defense process, data state perspectives, contextual issues, and protective mechanisms.

(g) Gathering historical information on previous detected incidents and situational specifics.

Automated, semi-automated, and manual reviews of information systems and infrastructures will be undertaken to include but not be limited to:

(a) scans of networks and address spaces to detect the structure and makeup of the network including any components that may be present and are not known to management and network connections that create external access and are not otherwise documented,

(b) scans of systems to identify widely known and published vulnerabilities,

(c) identification of services present on computers and the mapping of those services into expectations associated with the functions of those systems,

(d) penetration tests of key high consequence systems to identify the potential for external attacks on those systems and to determine potential effects of insiders attempting to gain unauthorized internal access,

(e) evaluation of select applications and infrastructure elements for understanding effects of risk aggregation on critical infrastructure elements,

(f) detailed internal examinations of select and representative systems to identify potential security issues. and

(g) other tests, reviews, demonstrations, or experiments as seen fit and approved for performance during the course of the review.

Other discussions, observations, and analysis as identified during the on-site visit will be collected for subsequent review and reporting.

2. FCA will provide a detailed review of what was observed and discussed at the site visit to CLIENT for its review. Typically this review is performed by sending individual information to those who participated in the effort so that they can review things they participated in and confirm or correct any results documented. CLIENT will respond to this information by returning comments from all parties in a consolidated form within 14 days of receipt of the material.

3. Following the receipt of responses from CLIENT, FCA will provide a draft report consisting of:

- An executive summary of the assessment
- A review of what was observed and discussed
- An assessment of CLIENT's protection posture based on that review
- Advised urgent, tactical, and strategic actions CLIENT should take
- Comparison of results against other comparable organizations
- A review of how CLIENT would likely perform against standards:
    - ISO17799
    - GAISP
    - COSO
    - CMM-SEC
    - or other standards as identified and agreed in advance.

If minor report revisions are required, they will be provided over a period of three months at no added cost. If an in-person executive briefing is desired, one will be provided at an additional cost of $5000 plus expenses.

This proposal is valid for a period of 45 days from the date provided. All payments are due within 15 days of invoice.

This proposal is valid for a period of 45 days from the date provided. All payments are due prior to scheduling of the assessment. Travel expenses will be

invoiced at the end of the site visit and are due and payable 15 days after invoice.

The cost of this assessment will be as specified in the pricing provided under separate cover.

Additional terms and conditions:

- **Single Point of Contact:** CLIENT will provide FCA with a single point of contact (SPOC) to coordinate all efforts associated with this task and that SPOC will be authorized and able to provide all necessary access and oversight including making on-the-spot decisions about activities to be allowed and refused as part of the IPPA. The SPOC will also be responsible to assure that FCA personnel are properly protected at all times, including interfacing with other security functions and knowledge of health and safety issues and will supervise all FCA activities or assign appropriate personnel to supervise specific technical activities as appropriate to the need.
- **Timely access:** CLIENT will provide timely access to all personnel, systems, facilities, information, and other materials, people, or things that are needed by FCA to perform the IPPA.
- **Timely response:** CLIENT will respond in a timely fashion to all requests for information and to draft reports and information. Failure to reply in a timely fashion will be treated by FCA as an inability to respond or a tacit agreement to information provided for feedback and FCA will continue its efforts under those assumptions. Changes after subsequent work may result in additional fees.
- **Liability limitations:** CLIENT indemnifies FCA and holds FCA harmless for all costs and consequences, whether direct or indirect, arising out of the IPPA, in all jurisdictions, in all forms, and in all cases.
- **Best efforts:** FCA will undertake best efforts to perform its tasks using the most suitable available technologies in a manner consistent with current usage, methodologies, techniques, and knowledge, however, because of the ever changing nature of the security, technology, business, regulatory, and physical environment, FCA MAKES NO WARRANTY, EITHER EXPRESSED OR IMPLIED, AS TO THE RESULTS OF THESE EFFORTS.
- **Confidentiality:** All CLIENT information is held in strictest confidence by FCA and its team members and all FCA techniques, processes, and activities are to be held in strictest confidence by CLIENT team members. Confidentiality, however, can be broken through court orders or other legal means. In such cases, all parties will seek to minimize exposure of confidential information wherever feasible. If payment of all fees related to the IPPA are not made in a timely fashion, confidentiality requirements and other related contractual obligations are no longer binding upon FCA and ownership of all results of the IPPA become the property of FCA.
- **Exceptions to confidentiality:** In some cases, FCA personnel encounter

contraband, such as images that may indicate the presence of child pornography, evidence of crimes, or observation of crimes in progress. In such cases as FCA management, at its sole discretion, may determine that there is a legal responsibility to report to authorities. In such cases FCA personnel will make such reports are are mandated by law. Client holds FCA harmless for all reporting made in such cases.

- **Ownership of results:** With the exception of the report and draft reports provided to CLIENT by FCA, all materials used in the performance of an IPPA are the intellectual property of FCA and will remain so after the IPPA.
- **Expenses:** CLIENT will cover all reasonable and normal expenses to FCA within 15 days of invoice for those actual expenses accrued during the assessment. Invoices provided by FCA will be sufficient proof of expenses however, if expenses seem excessive, FCA will provide additional supporting documentation as needed.
- **Comparison study:** FCA will provide no information about the entities compared in the comparison study except that between 3 and 5 entities will be used and these entities will be comparable to the entity under review in general terms of size, reach, makeup, and business type. Notice of deviations from this requirement will be provided when no comparable entity is available for this purpose in that dimension of comparability. Comparisons will only be made against FCA ratings and comparisons may include rating from studies of different detail levels and over different time frames.
- **General:** If any part of this Agreement shall be found unenforceable under the applicable laws, the remaining parts of this Agreement shall remain in force. The proper law and venue for this Agreement shall be that of Alameda County, in the State of California, in the United States of America, and the parties submit to the jurisdiction of the courts of this venue in all matters related to this Agreement. Time is of the essence in this matter and all activities will take place in a timely fashion. This Agreement constitutes the entire agreement between the parties, and supersedes any previous agreements that may have existed between the parties before the signing of this Agreement.