

This rating should be considered fluid and should be assessed on a regular basis against intelligence reports and other information.

**2.11 Assessment Process**

The assessment process consists of analyzing intelligence alongside historical information to allow a rapid, high quality decision to be made. The process requires that intelligence and information be considered against six predetermined factors, namely:

- Existence
- Capability
- Intentions
- History
- Targeting
- Environment.

The results from each of these categories are detailed below to allow the level of threat facing the legal team to be identified and the appropriate response to be selected.

Members of the legal team should consider themselves potential targets for hostile agents wishing to make a statement, cause death, injury or serious disruption to the legal process. The rigorous assessment process is normally only applied to extraordinary situations, and the criminal threat meets that criteria.

2.11.1 Existence - The existence of hostile agents is clearly demonstrated by the level of drug activity and the access to and abundance of firearms in Barbados. Threats have already been made against the legal team. Not for the first time, hostile agents may reach out and attempt to intimidate the legal team in Canada, as well as Barbados.

2.11.2 Capability – Newspaper articles have reported that similar tactics have been utilized against plaintiffs involved in legal action with companies and individuals resident in Barbados. One of the more high profile stories involved a Canadian citizen, Mr. Niten Amersey, who after 10 years of litigation with the Government of Barbados, won a court order entitling him to \$2 million of company equipment. When Mr. Amersey tried to claim his property, he found that the government had sent the army to override the court order and reclaim the equipment. Another story concerned a bus accident. Newspaper journalists photographed the accident scene. When police arrived, they immediately confiscated the reporter’s cameras and removed the film. There were further reports of physical abuse by the Police against the reporters.

2.11.3 Intentions – The Chief Justice of Barbados is a defendant in the legal action. His brother, Mr. Peter Simmons, has uttered threats to Mr. Stuart Heaslet, a witness in the proceedings, during a telephone conversation. It is expected that these threats would be carried out, particularly if the legal team deploy to Barbados.

2.11.4 Targeting - There is no specific targeting information against the legal team. The full extent of these issues will not become clear until the examination for discovery commences.

2.11.5 Recent History – The history of violence in Barbados is well documented. There is ample evidence to indicate a willingness by some defendants to employ all means at their disposal, including intimidation against witnesses and plaintiffs to subvert the course of justice and threats



of violence. The combination of more aggressive means of intimidation combined with a greater focus on the legal team could mean that eventually some type of action will be directed at the legal team either in Canada or Barbados.

2.11.6 Environment – At present, there is an active gun culture in Barbados and every type of firearm is readily available to anyone who can afford it. The legal team has recognized a potential problem and is mitigating some of the threats posed by potential hostile agents by having a threat assessment conducted. They are cognisant of the fact that prior preparation and planning will prevent an ineffective response. Plans to respond to future attacks should be developed and tested.

**2.12 Hostile Agent Activity in Barbados**

Drug gangs are a problem in Barbados. It is also possible that drug and criminal gangs operating in Barbados could reach out and touch members of the legal team through their proxies in Canada. Toronto has a large Caribbean community and the legal team should not consider themselves to be immune from potential threats or violence while in Canada.

**2.13 Threat Impact**

The TRVA has identified vulnerability and impact events so that appropriate mitigation measures can be developed.

A Security team can successfully mitigate the impact of most worse case and credible scenarios by ensuring it has effective physical security measures to reduce the probability of the event occurring and a competent team capable of reacting to incidents. This would significantly reduce the impact of a major security/criminal incident involving legal team activities.

Those threat events that would result in the greatest impact at each area are listed in the tables below.

The threat impact is based on potential damage to legal team activities from hostile agents. The magnitude of the event is measured by the impact on the continued operation of the business and is scored in the range of 1 - 5.

These are as follows:

- Catastrophic (5)
- High Impact (4)
- Medium Impact (3)
- Low impact (2)
- Negligible Impact (1)

2.13.1 Catastrophic Events - These are primarily natural disasters or hostile agent events. They include:

- Hurricanes;
- Vehicle Improvised Explosive Device (VIED) bomb placed in or near the legal teams accommodation or discovery areas;

2.13.2 High Impact Events – These events are major external related conditions:

- Major fire at the legal team's accommodations or discovery areas;
- Small explosive device – Planted in/near the legal team's accommodations or discovery areas;
- Hostage taking;
- Theft of legal team proprietary information;
- Physical attack against legal team members;

2.13.3 Medium Impact Events – These events would be associated with hostile agent activity:

- Bomb threats directed at legal team's accommodations or discovery areas;
- Threatening phone calls – Directed at legal teams accommodations or discovery areas;
- Disgruntled defendant;
- Adverse media event;
- Compromise of legal team's accommodations or discovery areas security measures;
- Surveillance against legal team conducted by hostile agents;
- Computer hackers;
- Petty theft;
- Unauthorized access to legal teams accommodations or discovery areas;
- Small/Medium fire at legal teams accommodations or discovery areas;
- Personal duress alarm requiring response;
- Medical emergency;
- Loss of communications.

2.13.4 Low Impact Events – These events could be experienced on a relatively common basis:  
Nil

2.13.5 Negligible Impact Events – These events could be experienced on a relatively frequent basis:  
Nil

## 2.14 Identified Impact Vulnerabilities

The TRVA has identified a comprehensive list of impact vulnerabilities to assist in the identification of risk events. Each vulnerability that has been identified has been assigned a risk level of Catastrophic – High Impact – Medium Impact or Low Impact. Additionally, the risk profiles have been classified by category and area.

- Catastrophic - Significant liability or risk exists which should be addressed immediately
- High Impact - Liability or risk exists which should be addressed as soon as possible
- Medium Impact - Liability or risk exists which should be addressed in the normal course of events
- Low Impact – no risk or liability exists

5 – Catastrophic

4 – High Impact

3 – Medium Impact

2 – Low Impact

A summary of impact vulnerabilities is provided below.



Vulnerability	Catastrophic	High Impact	Medium Impact	Low Impact
Hurricanes	5	-	-	-
Vehicle Improvised Explosive Device (VIED) bomb placed in or near the legal team's accommodation or discovery areas	5	-	-	-
Major Fire at the legal team's accommodations or discovery areas	-	4	-	-
Small Explosive Device – Planted In/Near the legal team's accommodations or discovery areas	-	4	-	-
Hostage Taking	-	4	-	-
Bomb Threats directed at legal team's accommodations or discovery areas	-	-	3	-
Threatening Phone Calls – Directed at legal team's accommodations or discovery areas	-	-	3	-
Disgruntled defendant	-	-	3	-
Loss of Radio Communications	-	-	3	-
Adverse Media Event	-	-	3	-
Compromise of legal team's accommodations or discovery areas security measures	-	-	3	-
Surveillance against legal team conducted by hostile agents	-	-	3	-
Computer Hackers	-	-	3	-
Petty Theft	-	-	3	-
Theft of legal team Proprietary Information	-	4	-	-
Unauthorized Access to legal team's accommodations or discovery areas	-	-	3	-
Major Accident during transportation of the legal team	-	-	3	-
Small/Medium Fire at legal team's accommodations or discovery areas	-	-	3	-
Physical Attack Against legal team members	-	4	-	-
Personal Duress Alarm Requiring Response	-	-	3	-
Medical Emergency	-	-	3	-

## 2.15 Threat Probability

The risk assessment determines the probability of the threat event occurring. It is rated from 5 (guaranteed) to 1 (not credible) and is based on historical information and intelligence assessments.

- Guaranteed – (5)
- High probability – (4)
- Medium probability – (3)
- Low Probability – (2)
- Non-Credible – (1)

In conducting this analysis, the consultant reviewed the possible vulnerabilities of the region. From this, and interviews with individuals, a listing of possible illegal and/or criminal incident types was generated. In order of likelihood, these incident types were categorized as follows:

### 2.15.1 Guaranteed Events

Nil

### 2.15.2 High Probability Events

- Trespassing into legal team's accommodations or discovery areas;
- Threatening Phone Calls – directed at legal team;
- Surveillance against legal team conducted by hostile agents;

### 2.15.3 Medium Probability Events

- Computer Hackers;
- Loss of legal team's proprietary information;
- Major Accident during transportation of the legal team;
- Compromise of legal team activities;
- Unauthorized Access to legal team's accommodations or discovery areas;
- Bomb Threats – directed at legal team activities;
- Loss of legal team's proprietary information;
- Attack in the vicinity of a legal team's accommodations or discovery areas;
- Loss of Radio Communications;
- Hostage Taking.

### 2.15.4 Low Probability Events

- Major Fire at legal team's accommodations or discovery areas;
- Physical Attack Against a legal team member;
- Small/Medium Fire at legal team's accommodations or discovery areas;
- Medical Emergency -
- Hurricanes (depending on time of the year);
- Robbery;
- Adverse Media Event;
- Small Explosive Device planted in or near a legal team's accommodations or discovery areas;
- Vehicle Bomb Placed in or near a legal teams accommodations or discovery areas;

## 2.16 Identified Probability Vulnerabilities

The TRVA has identified a comprehensive list of identified probability vulnerabilities to assist the security team in identifying risk probability events. Each event that has been identified by the consultant has been assigned a risk level of Guaranteed – High Probability – Medium Probability - Low Probability. Additionally, the risk profiles have been classified by category and area.

- Guaranteed - Significant risk exists which needs to be addressed immediately
- High Probability - Risk exists which should be addressed as soon as possible
- Medium Probability - Risk exists which should be addressed in the normal course of events
- Low Probability – No risk currently exists

5 – Guaranteed

4 – High Probability

3 – Medium Probability

2 – Low Probability

A summary of probability vulnerabilities is provided below.



Vulnerability	Guaranteed	High Probability	Medium Probability	Low Probability
Trespassing into legal team's accommodations or discovery areas;	-	4	-	-
Physical Attack Against a legal team member	-	-	3	-
Threatening Phone Calls – directed at legal team	-	4	-	-
Surveillance against legal team conducted by hostile agents	-	4	-	-
Computer Hackers	-	-	3	-
Loss of legal team's proprietary information	-	-	3	-
Major Accident during transportation of the legal team	-	-	3	-
Compromise of legal team activities	-	-	3	-
Unauthorized Access to legal team's accommodations or discovery areas	-	-	3	-
Bomb Threats – directed at legal team activities	-	-	3	-
Disgruntled defendant	-	-	3	-
Petty Theft	-	-	3	-
Compromise of legal teams accommodations or discovery areas	-	-	3	-
Personal Duress Alarm Requiring Response	-	-	3	-
Attack in the Vicinity of a legal team's accommodations or discovery areas	-	-	3	-
Major Fire at legal teams accommodations or discovery areas	-	-	-	2
Small/Medium Fire legal team's accommodations or discovery areas	-	-	-	2
Medical Emergency	-	-	-	2
Loss of Radio Communications	-	-	3	-
Hurricanes	-	-	-	2
Robbery	-	-	-	2
Adverse Media Event	-	-	-	2
Major Accident during transportation of the legal team	-	-	3	-
Small Explosive Device planted in or near a legal team's accommodations or discovery areas	-	-	-	2
Vehicle Bomb Placed in or near a legal teams accommodations or discovery areas	-	-	-	2
Hostage Taking	-	-	3	-



### 2.17 Threat Assessment

For each threat event, a probability ranking and an impact ranking are assigned based on the definitions above. The overall risk factor is calculated by multiplying the probability ranking by the impact ranking. Risk factor values between 1 and 5 are a low impact or infrequent occurrence such that they can be ignored from a planning perspective. Risk factor values between 6 and 10 have a probability of occurring and when they do, they will have such an impact that a response plan, including the necessary supporting systems, is required to effectively deal with the event.

Risk factor values between 11 and 25 have a high probability of occurring and have such a sufficient impact that they would cause serious loss to the company, and therefore mitigation actions should be taken to reduce severity. The range of possible risk factor values is described below.

### 2.18 Overall Risk Summary

Worse-case credible scenarios that may impact the legal team; include hostage taking (with a raw risk factor of 16) a physical attack against the legal team (with a raw risk factor of 14), threatening phone calls, surveillance of legal team, theft of proprietary information, unauthorized access to legal team, attack in the vicinity of the legal team (with a raw risk factor of 12).

A confluence of these threats could serve to magnify their impact and will have such an effect that a response plan, including the necessary supporting systems, is required to effectively mitigate these risks. In general, decreasing vulnerability can reduce the risk of a threat. There are three types of vulnerabilities that contribute to the risk of a potential threat. The types of vulnerabilities and current state of the legal team are identified below:

Environmental Vulnerabilities – There are no significant environmental vulnerabilities for the legal team, although damage could be caused by severe weather events such as a hurricane or local security problems associated with operating a hotel.

Physical Vulnerabilities – All security team activities within the hotel can be reasonably controlled. The same cannot be said for activities conducted outside the hotel. All external movement should be limited and, if required, should be spontaneous and involve the use of local taxis.

Risk Profile - The overall risk profile for the legal team’s activities is presented below, illustrating the risk assessment by category. In the risk profile, a risk rating is assigned to each of the risk categories based on the consultant’s findings; the higher the risk rating, the greater the vulnerability.

### Threat, Risk, Vulnerability Risk Summary

Threat Classes – Summary	Raw	Adjusted	Residual
<b>Internal</b> – The internal threat could emanate from an externally coerced, disgruntled or intimidated legal team member, witness or plaintiff.	Low	Low	Low
<b>External</b> – As a result of threats already made, the external threat is evident.			
<b>Economic</b> – The economic impact on the legal team could be considerable in the event witnesses and plaintiffs are threatened or coerced.			
<b>Criminal</b> - The awareness to overall threat from hostile agents will continue to increase as the legal action continues and it should be anticipated that it would continue to elicit response from hostile agents.			

Green (1-5)	Acceptable Loss Exposure
Yellow (6-10)	Response Plan Should Exist
	Mitigating Actions Should Exist

### Vulnerabilities

<b>Environmental</b> <ul style="list-style-type: none"> <li>Severe weather events such as a hurricane (depending on season).</li> </ul>	Low Risk
<b>Physical</b> <ul style="list-style-type: none"> <li>Local security problems associated with the operation of a hotel.</li> <li>Physical security within the hotel can be reasonably maintained, but not guaranteed.</li> <li>Restricting access to the legal team can be controlled, but not guaranteed.</li> <li>All external movement should involve use local taxis and be spontaneous.</li> </ul>	Medium Risk



## Threat, Risk, Vulnerability Assessment - Risk Profile

Threat	Probability	Impact	Raw Risk <sup>1</sup>	Impact of Recommendations <sup>2</sup>	Residual Risk <sup>3</sup>
Hurricanes	2	5	10	N/A	10
Vehicle Improvised Explosive Device (VIED) bomb placed in or near the legal team's accommodation or discovery areas	2	5	10	3	7
Major Fire at the legal team's accommodations or discovery areas	2	4	8	3	5
Small Explosive Device – Planted In/Near the legal team's accommodations or discovery areas	2	4	8	2	6
Hostage Taking					
Bomb Threats directed at legal team's accommodations or discovery areas	3	3	9	3	6
Threatening Phone Calls – Directed at legal team's accommodations or discovery areas					9
Disgruntled defendant	3	3	9	3	6
Adverse Media Event	2	3	6	2	4
Compromise of legal team's accommodations or discovery areas security measures	3	3	9	2	7
Surveillance against legal team conducted by hostile agents					9
Computer Hackers	3	3	9	2	6
Petty Theft	3	3	9	2	6
Theft of legal team Proprietary Information					9
Unauthorized Access to legal teams accommodations or discovery areas					9
Loss of Communications	3	3	9	3	6
Small/Medium Fire at legal team's accommodations or discovery areas	2	3	6	2	4
Physical Attack Against legal team members					11
Personal Duress Alarm Requiring Response	3	3	9	3	6
Medical Emergency	2	3	6	2	4
Major Accident during transportation of the legal team	3	3	9	3	6
Attack in the Vicinity of a legal team's accommodations or discovery areas					9
Vehicle Bomb Placed in or near a legal team's accommodations or discovery areas	2	4	8	2	6

- <sup>1</sup> Raw Risk – current risk (probability times impact) based upon existing security programs.
- <sup>2</sup> Impact of recommendations – Should all recommendations be implemented and security programs developed, the raw risk would be reduced by this amount – note: this is a subjective analysis and based upon circumstances known and present at time of review.
- <sup>3</sup> Residual Risk – Remaining risk exposure



**Section Three**

**KEY OBSERVATIONS AND FINDINGS**

**Operational Overview**

The legal team should consider themselves potential targets from unidentified hostile agents either resident in or associated with Barbados. Motivation for attacks could be political and/or social and stem from hostile agents directed by persons unknown with the intent to threaten (i.e. physical or bomb), vandalize, intimidate, physically assault, kidnap or murder members of the legal team or their families. In addition to the individuals targeted, the law firm could suffer collateral damage through loss in productivity, bad publicity, loss of credibility, legal decision slow down and possible loss of client confidence. A paid or threatened hostile agent will always be a potential threat.

There are a number of areas that are vital to the safety and security of the legal team and should be protected at all times. If penetrated, these areas could seriously impact the safety and security of the legal team. The deployment of trained security manpower and development of specific procedures should be put in place to ensure security for these areas.

On July 19 2007, the Canadian Prime Minister visited Barbados, where he committed to strengthening the Canada-Barbados relationship. At the same time, he announced that Canada would be making an important contribution of computer equipment and training to assist in the development of the defence and security capacity of CARICOM countries. The Government of Barbados, as a result of this meeting, has agreed to partner in the Canadian Manufacturers and Exporters Association conference being held in Barbados in January, 2008.

Prior to the Prime Minister's arrival, his RCMP protection team completed a comprehensive risk assessment, determined that there were no direct threats and elected not to carry firearms.

On Friday, October 12, 2007 the consultant attended a meeting at the Canadian High Commission in Barbados with Charlotte Blumenshein, Political and Public Affairs Officer and Douglas Holland, Counsellor (Political and Economic Relations and Public Affairs) for Barbados and the Eastern Caribbean.

While explaining that GRI had been retained to provide security for a group of Canadian VIP's travelling to and working for a short time in Barbados, Ms. Blumenshein asked if this was in relation to the Kingsland Estates action! She was fully aware of the circumstances surrounding this lawsuit and suggested that Douglas Holland be included in the meeting. Mr. Holland had only been working at the Canadian High Commission for three weeks, yet the Department of Foreign Affairs and International Trade (DFAIT) in Ottawa had already briefed him prior to his departure. Both individuals agreed that this was a political "hot potato" and the ramifications could include "bringing down" the existing government, its loss of credibility and possible criminal charges if wrongdoing was ever proven. Both agreed that a fair hearing in the Barbadian justice system, under the circumstances, could prove difficult, particularly as the Lord Chief Justice is involved as a defendant. It was suggested that the best course of action would be to conduct examinations for discovery in Canada, thereby assuring full, unbiased judicial process.

The rumours of corruption at the highest level in Barbados within the government are rife.



This impending action has received extensive media coverage in Barbados, especially by the Barbados Free Press, an independent media resource, which maintains an Internet blog site at [www.barbadosfreepress.com](http://www.barbadosfreepress.com). The consultant discovered many articles relating to the government, its activities and numerous mentions of some of the defendants. While it is impossible to corroborate all the articles posted, even if only a small percentage is factual, there is considerable room for concern as well as further investigation.

The consultant was informed that the Barbadian Prime Minister currently owns a multi-million dollar home in a select enclave on the west coast of Barbados, well beyond the means of his salary. While challenged on this fact in the media, he has declined comment. Recently, the Head of Customs was found to have a multi-million dollar bank account in the CIBC bank in Bridgetown. On March 25, 2007, the Tourism Minister stormed out of a radio interview when asked how he became a millionaire in such a short time on a government salary.

The government is required to go to the polls late this year or early 2008 and it is anticipated that they will not be successfully re-elected. Although not proven in court, Barbadians speculate that the majority of senior level politicians have spent the past five years of their 15 years in power lining their pockets in anticipation of their defeat. Several officials have been involved in business dealings that, while they have been in power, appear to have accumulated a significant amount of wealth. This information is based purely on rumour and speculation.

On April 29, 2007, Mr Albert Brandford, a political correspondent, wrote, "most of the stealing in government takes place where government interfaces with the private sector of Barbados. You can't steal salaries and you can't steal debt payments". For more information regarding this article please see Appendix D.

Following were amongst the more critical findings that were identified during the review, conducted October 10-14, 2007.

### 3.2 Examination for Discovery Options

Three facilities were pre-identified as potential locations for the legal team to conduct examinations for discovery and each were visited and reviewed by the consultant.

The three locations reviewed were the Hilton Barbados Hotel, the Inn Chambers and Manor Lodge.

#### 3.2.1 Hilton Barbados Hotel

The Hilton Barbados Hotel is located three (3) miles from Bridgetown and eighteen (18) miles from The Grantley Adams International Airport. The Hilton is a four star hotel and provides all the amenities that one would expect from an international Hilton. Located at Needhams Point, it is isolated at the end of a single road from the main highway between the airport and Bridgetown. This reflects positively for security, as all vehicle and pedestrian traffic can be monitored moving in and out of the hotel. A CCTV camera and a gatehouse, manned 24/7, also cover this entrance road.

The hotel has a 24-hour private security guard presence provided by Group 4 Securitas, a locally contracted guard company. Group 4 Securitas are a global security company who typically, in most countries, have high standards of training. They also provide security for the international airport.



CCTV cameras are deployed throughout all public areas, both internally and externally.

External CCTV cameras are mounted on the roof of the hotel buildings covering the driveway, car parking area, beach and pool areas. Internal CCTV cameras are placed to cover the majority of public areas on the hotel's ground floor.

All CCTV cameras appear to be fixed; although it is not known if they have a Pan-Tilt-Zoom (PTZ) capability, as during the review, they were not noticed to change viewing positions. It is also not known whether these CCTV camera systems are physically monitored or recorded. As expected, there is an extensive life safety system throughout the hotel, including smoke detectors, fire pull stations, magnetic locked fire doors, fire sprinkler systems, fire extinguishers and trained hotel staff. The hotel's perimeter is surrounded by a six-foot high wire fence topped with barbed wire. Vehicle and pedestrian access control by the gatehouse guard is limited and most vehicles and pedestrians have unimpeded access onto the hotel property.

The hotel offers two towers for guest accommodation, namely: The Lighthouse Tower (facing the main beach) and the Fort Tower, (facing Bridgetown).

A 10,000 square foot conference facility, including banquet and conference rooms is operated on the lower level of the hotel. There are a number of conference rooms suitable for use by the legal team to conduct examinations for discovery. All conference rooms have soundproofed sliding panelled walls for separation and are equipped with integrated sound and data cabling systems. Conference rooms provide outdoor access to a covered terrace.

The hurricane season commences in June and ends in November. Barbados has not suffered a full hit by a major hurricane for over 27 years because of its location, although it does experience peripheral activity, the last being a brush with Hurricane Denis in 2007. The hotel is owned by the government of Barbados and managed by the Hilton Hotel Group. The general manager of the hotel is a Canadian citizen who is alleged to have an excellent relationship with the Canadian High Commission.

Recommendations

- The Hilton Barbados would provide a location for the legal team to stay and conduct its examinations for discovery.
- The legal team should be located on a lower floor (ideally the second floor) to permit easy evacuation from the hotel in the event of an incident. Their rooms should be blocked together, running consecutively from room 201 to 204 to facilitate access control by the security team, who would occupy rooms 205-209. A fire escape is located opposite room 201, which would facilitate a quick evacuation if required.
- High season runs from November to the end of April and it is anticipated block-booking rooms at this time may prove difficult.

A trained security team could secure and monitor rooms utilized by the legal team throughout the hotel complex without attracting undue attention.

3.2.2 Inn Chambers

Inn Chambers is an active legal office located on Lucas Street, between James and Swan Streets in the centre of Bridgetown. It is 200 metres from the main tourist shopping areas on Broad Street and 200 metres from the Barbados Law Courts and Central Police Station.

The area itself is built up around tourist related retail, commercial and residential properties. Situated on a northbound one-way street, Lucas Street houses the Inn Chambers, Law Courts and Central Police Station.



The building is three storeys and a plaque on its facade identifies it as a "Barbados Natural Trust building of architectural interest". Incorporated into its facade at the side is a passageway leading to the rear of the building where there is parking for six (6) vehicles.

Although parking is restricted on both sides of Lucas Street because it is one way and very narrow, its signage is largely ignored and at the time of the review, there were numerous vehicles parked directly outside the building significantly limiting access into it. The building is overlooked by adjacent properties both at the front and rear.

The following attorneys are listed as practicing law from the Inn Chambers:

- Alair Sheppard
- M. Adrian King
- Peta-Gay Lee Brace
- Wendy Maraj
- Dyon Scarlett
- Lisa A. Gaskin
- Varia Williams
- Desmond D. Sands
- Philip McWatt
- Kareen Cole
- M. Tariq Khan

Recommendation

- This building is unsuitable for discovery examinations and is not recommended because of its location and lack of escape routes. Although it is in close proximity to the law courts, the area is extremely busy and many of those individuals attending court proceedings would pass in close proximity to its facade. The daily drive to and from the hotel down small, narrow and congested streets, combined with parking and securing of team vehicles, would be difficult. The building provides two possible exits, both leading onto Lucas Street. Protection of the legal team and the ability to effect a rapid evacuation in the event of an incident may be problematic.

3.2.3 Manor Lodge

Manor Lodge is located fifteen (15) miles north of Bridgetown between the parishes of St Thomas and St Michael. It is best described as a large, multi-use business complex. There are two main buildings labelled A and B and a number of external buildings housing diverse business entities. This area is somewhat isolated from Bridgetown and is in close proximity to a large residential area called Eden Lodge. The complex is consistently busy with vehicles and pedestrians moving in and out of the various business units.

A security hut is located at the entrance of the Manor Lodge "A" building, but it was unoccupied at the time of review and no additional security presence was evident. Vehicle access is not controlled and over 27 vehicles were parked inside and on the periphery of the complex. The legal office of interest was located directly behind the Exclusive Lighting store in a single storey building. It took the consultant over fifty (50) minutes to drive to Manor Lodge from the hotel in heavy traffic.



### Recommendation

- This location is unsuitable for examination for discovery proceedings because of its isolated location, the amount of activity in the complex and the travel distances that would be involved on a daily basis.

#### 3.2.4 Renting of a Local Villa

During the review, the option of renting of a villa for the legal team was explored. The majority of villas are located along the coast in relatively isolated locations, some way from Bridgetown. Response to these areas would be lengthy and it would be impossible for an unarmed security team to provide any level of protection. Extended drive times would also present major vulnerabilities, particularly along narrow roads and, in some cases, tracks to/from offices where examinations for discovery would be taking place. It is not recommended that the legal team consider this option.

### Recommendation

- The renting of a villa to accommodate the legal and security teams is unadvisable. Securing an isolated location can be problematic. Vulnerabilities increase when extended periods of time must be spent driving in heaving traffic.

### 3.3 Security Considerations

#### 3.3.1 Access Control

Access control can be described as the entry/exit regulation of individuals through controlled points. Regardless of the environment involved, it is desirable to have as few access control points as possible, in order to achieve maximum levels of security and cost effectiveness.

During the review, it became evident that access to legal team internal areas will be easily attainable, as they will be located in a hotel environment.

There are numerous ways to gain physical access into protected environments:

- Direct access into public areas;
- Use of static surveillance;
- Hiring a legal team employee who has the specific knowledge desired;
- Bribing or coercing a hotel employee, driver, legal clerk;
- Stealing of proprietary legal documentation (i.e. schematics, documents, garbage, or magnetic media or policies and procedures);
- Planting a "mole" in the legal team, whose true identity is hidden and whose task is to compromise the legal proceedings, access the legal team's computer files and intercept all communications with the aim of gaining legal team confidential information;
- Using the services of third parties for blackmail purposes;
- Using the services of a third party to develop a close personal relationship with a legal team member known to have access to confidential information or direct access to restricted areas.



Other non-intrusive methods include:

- The use of open source information in an attempt to gather legal team confidential information;
- Obtain research materials (i.e. other client information, reports and analyze legal team past performances in similar type of legal actions);
- General disclosures made by existing/former legal team members or clients.

Recommendation

- Ensure that access to the legal team is controlled 24/7.

3.3.2 Accommodation Security

Consideration should be given to restricting access to the legal team's hotel rooms and other identified areas through the positioning of static Personal Protection Officers (PPO). A PPO would secure all access doors to accommodations and the examination for discovery areas. Hotel housekeeping would be required to request access to the legal team's rooms from the security team and would be supervised while they carried out their duties.

Security measures will be principally aimed at achieving a minimum level of access control to the legal team. Hotel floor security is weak, as security staff does not effectively monitor individuals entering or leaving the elevator lobby area. All hotel staff wear identifiable uniforms and it would be relatively easy to identify somebody who does not "fit in". It may be possible to have a member of the hotel management verify housekeeping staff requiring access into the legal teams accommodation. The security team would conduct a formal search of all legal team rooms and secure same 24/7 if required. It will be essential that once the rooms have been searched and declared clear of possible illegal substances and listening devices that the rooms are monitored by a member of the security team.

Recommendations

- Visitors to the legal team's floor space should be identified prior to entering the area;
- Deploy security 24/7 to monitor hotel rooms.

3.3.3 Driving In Barbados

Research indicates that 70% of the risk occurs usually while the individual is in transit, particularly within half a mile of a residence or office. If the legal team requires transportation, taxis should be utilized.

The renting of vehicles will add another layer of vulnerability to the legal team's safety and security, primarily because the vehicles would be left unattended for extended periods. Unsupervised, parked vehicles can be sabotaged, vandalized, be tagged with listening or tracking devices or planted with illegal substances by hostile agents. If set up for possession of an illegal substance, the legal process and credibility of the team would be placed in serious jeopardy.

There are no detailed road maps available in Barbados and the majority of roads are not clearly marked rendering it virtually impossible for an outsider to navigate successfully. The hiring of a dedicated local driver and vehicle is also not recommended, primarily because it will be impossible to determine their level of training and whether or not they are planted hostile agents.



If local taxis are utilized at any time, there should be no discussion of legal matters or proceedings in the taxi, as they may be under surveillance. If a member of the legal team leaves the hotel in a vehicle, it is possible that he/she will be followed.

If a decision is made to rent vehicles and assign a member of the security team with driving responsibilities, the driver will be trained to conduct counter surveillance and have formal security related training.

Access into the hotel car parking area is public and uncontrolled. There is one CCTV camera monitoring the car park from the roof of the Fort Tower.

#### Recommendation

- The legal team should not rent vehicles and should utilize local taxis if required to travel outside the hotel.

### 3.3.4 Vehicle Rental Agencies

Barbados has many vehicle rental agencies, but they are local to Barbados and not known out-of-country. Unfortunately, there are no established international agencies represented in Barbados. This could pose a security problem when renting, as vehicles could be compromised by hostile agents. If rental vehicles are utilized, they will need to be thoroughly searched and monitored by security 24/7 while in use.

### 3.3.5 Communications

The availability of sophisticated cell phone monitoring equipment implies that extreme care be used when team members use their phones, particularly when calling out-of-country. Care will also need to be exercised if using hotel room and public phones in the hotel lobby. Random use of public phones does permit a level of security, but once again, care should be taken and the legal team should consider that conversations they have are being monitored and act accordingly.

Local cell phones should be rented to permit communication between the legal and security team.

#### Recommendations

- Cell phone protocols should be developed and adhered to prior to leaving Canada.
- Local phones utilizing international and domestic phone chips should be used once deployed in Barbados.

### 3.3.6 Security of Documentation

It will be the responsibility of all members of the legal team to manage their own hardcopy documentation. All documentation surrounding legal proceedings and laptop computers are considered sensitive and will need to be secured 24/7. Housekeeping staff should be supervised while carrying out their duties.

Careful consideration must be applied, especially in discovery rooms, as defendants and their counsel will also be accessing these areas on a regular basis.



### Recommendations

- Consider depositing sensitive legal documents at the Canadian High Commission;
- Security will secure all sensitive documentation at the end of each day's proceedings.

#### 3.3.7 Confidential Documentation

All confidential legal documentation will need to be secured 24/7. Protocols for the shredding of confidential information while in Barbados should be considered prior to departure. All documentation relevant to legal proceedings should be transported back to Canada in carry on luggage.

### Recommendations

- All confidential documentation should be retained, kept secure and carried back to Toronto in carry-on luggage on completion of the trip
- A decision as to whether all documents will be returned to Canada on completion of the examination for discovery or some disposed of (shredded) in Barbados needs to be considered.

#### 3.3.8 Electronic Surveillance and Counter Measures

Unless secured 24/7 by security, the legal team's rooms and conference room work spaces will need to be swept for electronic devices on a daily basis. A protected environment is necessary so the legal team can discuss sensitive legal matters without fear of compromise.

Eavesdropping is most commonly achieved through wiretapping, bugging and the interception of cellular telephone conversations and local computer systems through hacking into modems and network devices.

Meetings can be compromised through the deployment of telephone taps, tape recording machines or the use of parabolic laser microphones pointing into conference rooms and areas from adjacent windows or roofs. Wiretapping pertains to the interception of information transmitted via a telephone line, including phone conversations, facsimile and computer transmissions. Because detection is difficult, the extent of the problem is impossible to gauge. Electronic eavesdropping technology is so highly developed that countermeasures have barely kept pace. Consequently, only the most expertly trained, equipped and experienced technician can counter the threat. An electronically minded individual may purchase all the equipment necessary to manufacture a sophisticated device from local electronics supply stores. Daily checks for listening devices should be conducted on the legal teams rooms, conference areas and other identified locations. These checks should include both physical and electronic countermeasures.

To prevent compromise through electronic interception and enable the legal team to work uninhibited, an active Technical Surveillance Countermeasures (TSCM) program will be required. The possibility for electronic compromise exists at all locations reviewed.

### Recommendations

- An Electronic Technical Surveillance Countermeasures program should be considered.
- An Electronic Technical Surveillance Countermeasures technician should be deployed with the security team.